

МЕЖДУНАРОДНАЯ ИНТЕГРАЦИЯ В СФЕРЕ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ НА ПОСТСОВЕТСКОМ ПРОСТРАНСТВЕ

В настоящей статье раскрываются вопросы интеграции законодательства в сфере уголовно-правовой защиты компьютерной информации и борьбы с киберпреступностью. Проводимым анализом Конвенции о преступности в сфере компьютерной информации (ETS N 185) и Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации определяются возможности сотрудничества государств в данной сфере.

Ключевые слова: киберпреступность, преступления в сфере компьютерной информации, интеграция, информационная сфера.

V.M. Elin

INTERNATIONAL INTEGRATION IN THE SPHERE OF CRIMINAL-LEGAL PROTECTION OF COMPUTER INFORMATION ON POST-SOVIET SPACE

This article describes the problems of integration in the criminal law – legal protection of computer information and the fight against cybercrime. The analysis of the Convention on Cybercrime information (ETS N 185) and the Agreement on Cooperation among States – members of the Commonwealth of Independent States in combating crimes in computer information identifies opportunities for cooperation among states in this area.

Keywords: cybercrime, cybercrime information integration, information environment.

В настоящее время значительное внимание в вопросах международной интеграции в информационной сфере уделяется проблеме борьбы с достаточно новым направлением высокоинтеллектуальной преступности – преступностью компьютерной, что требует сложных мер борьбы и усиления сотрудничества государств. Недаром Резолюцией Генеральной Ассамблеи ООН № 55/63 от 4 декабря 2000 г. определено, что:

– государства должны обеспечить, чтобы их законодательство и практика не оставляли возможности тем, кто злоупотребляет информационными технологиями, укрываться где бы то ни было;

– сотрудничество правоохранительных органов в расследовании случаев трансграничного преступного использования информационных технологий и судебном преследовании в этой связи должно координироваться всеми соответствующими государствами и т.п. [1].

При этом Резолюцией № 56/121 от 19 декабря 2001 г. государствам рекомендовано при разработке национальных законов, политики и практики в деле борьбы с преступным использованием информационных технологий надлежащим об-

разом учитывать работу и достижения Комиссии по предупреждению преступности и уголовному правосудию и других международных и региональных организаций.

Позднее Генеральной Ассамблеей ООН принята Резолюция № 58/199 от 23 декабря 2003 г. «Создание глобальной культуры кибербезопасности и защита важнейших информационных структур», в которой приняты к сведению элементы для защиты важнейших информационных инфраструктур; предложено всем соответствующим международным организациям, включая соответствующие органы ООН, в надлежащем порядке учитывать среди прочего эти элементы для защиты важнейших информационных инфраструктур в любой будущей работе по вопросам кибербезопасности или защиты важнейших инфраструктур; предложено государствам-членам учитывать среди прочего эти элементы при разработке своих стратегий уменьшения рисков для важнейших информационных инфраструктур в соответствии с национальными законами и нормами.

Таким образом, ООН выполняет значительную работу по проведению в жизнь концепции информационного общества. Для резолюций Генеральной Ассамблеи характерна высокая степень

¹ Доцент кафедры гражданско-правовых дисциплин НОУ ВПО «Российский новый университет».

обобщения существующих проблем информационного общества. Они подчеркивают значение концепции информационного общества для мирового сообщества в целом, а также для отдельных государств, гражданского общества и частного сектора. При этом ООН выделяет ключевые проблемы развития информационного общества, в том числе использование информационно-коммуникационных технологий в целях развития и кибербезопасность [2].

По мнению Широкова В.А., Беспаловой Е.В. [3] первая попытка разработки понятия компьютерного преступления была предпринята в рамках Организации экономического сотрудничества и развития (ОЭСР). С 1983 по 1985 г. Комитет ОЭСР обсудил возможность международной гармонизации уголовного законодательства отдельных государств с целью борьбы с экономическими компьютерными преступлениями. В 1986 г. Комитетом был предложен единый список действий, которые должны рассматриваться как компьютерные преступления в законодательстве государств-членов. В список были включены ввод, уничтожение, изменение, изъятие компьютерных данных, совершенные умышленно с намерением совершить незаконный перевод денежных средств и иных ценностей, аналогичные действия с целью совершить подделку компьютерной информации, воспрепятствование функционированию компьютерных систем, а также нарушения исключительных прав обладателей компьютерных программ с целью коммерческого использования, незаконное «прослушивание» компьютерных сетей и вмешательство в функционирование оборудования, предназначенного для обеспечения безопасности компьютерных систем.

В период с 1985 по 1989 г. над проблемой компьютерных преступлений работал Отдельный комитет экспертов по компьютерным преступлениям Совета Европы. По итогам работы Комитета 13 сентября 1989 г. Совет Европы принял Рекомендацию N R89(9) Комитета министров стран – членов Совета Европы о преступлениях, связанных с компьютерами. В ней определены практически все преступления, связанные с использованием компьютерных технологий, а также дана классификация компьютерных преступлений с рекомендуемым и факультативным перечнями для включения их в национальное законодательство.

По всей видимости, закономерным итогом указанной работы явилось принятие кодификатора Интерпола по компьютерным преступлениям 1991 года, согласно которому компьютерные преступления получили кодирующую литеру “Q” и разбиты на шесть основных классов следующим

образом: QA – Несанкционированный доступ и перехват; QD – Изменение компьютерных данных; QF – Компьютерное мошенничество; QR – Незаконное копирование; QS – Компьютерный саботаж; QZ – Прочие компьютерные преступления.

Естественно, процесс борьбы с данными преступлениями продолжает совершенствоваться до настоящего времени, примером чего выступает ряд нормативных актов, принятых международным сообществом и регулирующих уголовно-правовую защиту информационных объектов, к которым, в частности, можно отнести ряд конвенций Совета Европы: «О преступности в сфере компьютерной информации» 2001 года (ETS N 185), «О взаимной правовой помощи по уголовным делам в том, что касается судебных поручений о перехвате телекоммуникационных сообщений» NR (85), «О борьбе с пиратством в области авторского права и смежных прав» NR (88), «О порядке использования персональных данных полицией» NR (87), «О защите персональных данных в сфере телекоммуникационных услуг, в особенности телефонных услуг» NR (95), «О преступлениях, связанных с компьютерами» NR (89), Конвенции «По проблемам уголовно-процессуального права, связанным с информационными технологиями» NR (95)13.

Из указанного перечня документов особое внимание обращает на себя «Конвенция о преступности в сфере компьютерной информации» (ETS N 185), заключенная в Будапеште 23.11.2001, согласно положениям которой перечень мер в указанной сфере подразделяется на три категории: материальное уголовное право, процессуальное законодательство и юрисдикция. При этом следует иметь в виду, что к нормам материального уголовного права отнесены преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (включая противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование устройств); правонарушения, связанные с использованием компьютерных средств (подлог с использованием компьютерных технологий и мошенничество с использованием компьютерных технологий); правонарушения, связанные с детской порнографией, и правонарушения, связанные с нарушением авторского права и смежных прав.

Без сомнения, указанная Конвенция могла бы послужить значительным шагом к унификации законодательства в сфере борьбы с киберпреступностью, в т.ч. и на постсоветском пространстве, поскольку к ней помимо стран Европы и Америки

также присоединились страны Балтии, Украина, Армения, Азербайджан.

Распоряжением Президента РФ от 15.11.2005 № 557-рп [4] Россия приняла решение подписать Конвенцию с заявлением. Однако спустя несколько лет Распоряжением Президента РФ от 22.03.2008 № 144-рп Распоряжение Президента РФ от 15.11.2005 № 557-рп утратило силу без каких-либо объяснений.

Таким образом, Российская Федерация отказалась от возможности присоединения к 23 странам, осуществляющим совместную деятельность в указанной сфере. По всей видимости, причиной столь несолидного поведения послужила необходимость внесения изменений в действующее уголовное законодательство в части борьбы с преступлениями компьютерной информации, что, в свою очередь, могло бы повлечь сложности как в формулировке диспозиций статей, так и в правоприменительной сфере.

Интеграционный процесс на постсоветском пространстве в сфере борьбы с компьютерными преступлениями включает в себя как значительное количество двусторонних соглашений о сотрудничестве в области защиты информации между Российской Федерацией и государствами, входящими в состав СНГ [5], так и многостороннее «Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации», заключенное в Минске 01.06.2001 [6].

Анализ ст. 3 указанного Соглашения позволяет сделать вывод о том, что на момент его подписания уголовное законодательство Азербайджана, Армении, Белоруссии, Казахстана, Киргизии, Молдавии, России, Таджикистана, Узбекистана и Украины направлено на борьбу с умышленными противоправными деяниями в сферах осуществления неправомерного доступа к охраняемой законом компьютерной информации; создания, использования или распространения вредоносных программ; нарушения правил эксплуатации ЭВМ, систем ЭВМ или их сети; незаконного использования программ для ЭВМ и баз данных, являющихся объектами авторского права.

При этом следует иметь в виду, что только Азербайджан и Украина подписали Соглашение с оговорками, учитывающими национальное законодательство, национальные интересы и международные обязательства этих стран. Указанное обстоятельство указывает не столько на новизну пути данных стран в сфере уголовно-правовой защиты компьютерной информации, сколько на достаточно своеобразные диспозиции составов преступлений.

Так, Уголовный кодекс Украины, вступивший в силу 01 сентября 2001 года предусматривает уголовную ответственность за: «Незаконное вмешательство в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей» (ст. 361); « Хищение, присвоение, вымогательство компьютерной информации либо завладение ею путем мошенничества или злоупотребления служебным положением» (ст. 362); «Нарушение правил эксплуатации автоматических электронно-вычислительных систем» (ст. 363) и др [7].

Следует также иметь в виду, что интеграционный процесс стран постсоветского пространства в указанной сфере не ограничивается исключительно унификацией уголовного законодательства, поскольку ст. 5 Соглашения дополнительно предусматривает сотрудничество в следующих формах:

а) обмена информацией, в том числе:

– о готовящихся или совершенных преступлениях в сфере компьютерной информации и причастных к ним физических и юридических лицах;

– о формах и методах предупреждения, выявления, пресечения, раскрытия и расследования преступлений в данной сфере;

– о способах совершения преступлений в сфере компьютерной информации;

– о национальном законодательстве и международных договорах, регулирующих вопросы предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере компьютерной информации;

б) исполнения запросов о проведении оперативно-розыскных мероприятий, а также процессуальных действий в соответствии с международными договорами о правовой помощи;

в) планирования и проведения скоординированных мероприятий и операций по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации;

г) оказания содействия в подготовке и повышении квалификации кадров, в том числе путем стажировки специалистов, организации конференций, семинаров и учебных курсов;

д) создания информационных систем, обеспечивающих выполнение задач по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации;

е) проведения совместных научных исследований по представляющим взаимный интерес проблемам борьбы с преступлениями в сфере компьютерной информации;

ж) обмена нормативными правовыми актами, научно-технической литературой по борьбе с преступлениями в сфере компьютерной информации;

з) в других взаимоприемлемых формах.

Естественно, заключение указанного соглашения позволит расширить правовую базу сотрудничества правоохранительных и судебных органов государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации.

Таким образом, в настоящее время можно сделать вывод о том, что на постсоветском пространстве имеется тенденция к унификации законодательства в сфере уголовно-правовой защиты компьютерной информации, направленная, в первую очередь, на формирование единого информационного пространства, определяемого и регулируемого традиционно существовавшими и возникающими в настоящее время хозяйственными связями.

При этом следует иметь в виду, что процесс интеграции законодательства в сфере киберпреступности облегчается тем обстоятельством, что в развитии законодательства страны постсоветского пространства прошли общий путь развития, что, однако, не исключило определенного своеобразия.

Очевидно, что российскому законодателю следует оценить опыт зарубежных государств и выяснить пригодность вышеупомянутых правовых инструментов для защиты компьютерной информации.

Литература

1. <http://www.un.org/russian/documen/gadocs/gares.htm>.

2. *Талимончик, В.А.* Резолюции международных организаций в сфере информационного обмена // Информационное право. – 2006. – № 4.

3. *Широков, В.А., Беспалова, Е.В.* Киберпреступность: история уголовно-правового противодействия // Информационное право. – 2006. – № 4.

4. Собрание законодательства РФ. – 2005. – № 47. – Ст. 4929.

5. *Ястребов, Д.А.* Международно-правовое сотрудничество государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Юридический мир. – 2008. – № 12.

6. Собрание законодательства РФ. – 2009. – № 13. – Ст. 1460.

7. *Ястребов, Д.А.* Законодательный опыт стран – участниц Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Российский следователь. – 2008. – № 6.